```
function makehash(pw,mult) {
pass=pw.toUpperCase();
hash=0;
for (i=0;i<8;i++) {
letter=pass.substring(i,i+1);
c=alpha.indexOf(letter,0)+1;
hash=hash*mult+c;
}
return(hash);
}

//<![CDATA[
////WORK IN PROGRESS
//]]>
```

>//ACCESS GRANTED

HDDkey

The KEY for your undisturbed sleep...

user manual

WARNING!

HDDKEY is intended to be used with hard drives ONLY! DO NOT try to connect it to your CD-ROM or DVD-ROM. Connecting the HDDKEY to a device other than the HARD DRIVE can damage the HDDKEY!

There can be only one HDDKEY controlled hard drive on one IDE cable!

Do NOT connect any IEEE-1394 FireWire devices and do NOT connect your key token to the FireWire port!

CONTENT

FEATURES 3

1. Installation Overview 4
2. System Configurations 5
   - Image 1. The single hard drive in the system. 5
   - Image 2. Master drive encrypted, Slave drive not encrypted. 5
   - Image 3. Slave drive encrypted, Master drive not encrypted. 5
   - Image 4. Slave drive encrypted with master DVD recorder. 6
   - Image 5. Master drive encrypted with slave DVD recorder. 6
   - Image 6. 6
3. Connecting the KEY token 6
   - Image 7. 7
   - Image 8. 7
   - Image 9. Key tokens. 7
4. Preparing drives 8
5. More HDDKEY devices and only one secret key token 8
   - The 6pin header socket 9

SPECIFICATION 10

- 10 pin secret key header on the HDDKEY controller board. 10
- Power supply socket on the HDDKEY controller board. 10
- IEEE-1394 (FireWire) female socket on the controller board. 10
- 6 pin secret key header on the HDDKEY controller board. 10
- Jumper settings on the HDDKEY controller board. 11
- ULTRA ATA jumper settings on the HDDKEY controller board. 11

HDDkey

The KEY for your undisturbed sleep...

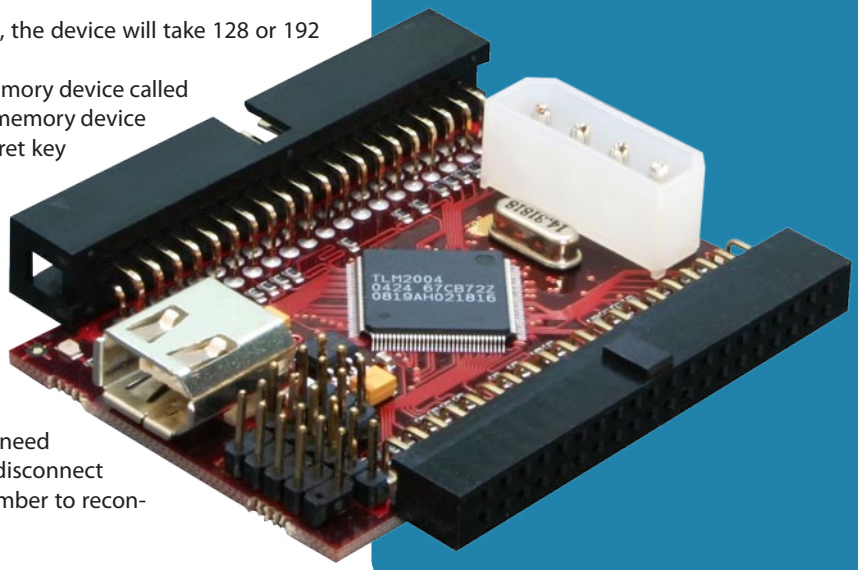
FEATURES

HDDKEY is a revolutionary device intended to encrypt in real time, the entire hard disk content, on the fly, without performance degradation. You will not notice that the device is attached. You will not notice any performance lose of your system. Everything on the hard drive is encrypted from the partition table, through the boot sector (MBR) to the operating system, swap file and all user files.

HDDKEY is a device specially designed to encrypt and decrypt data with the 3DES (Triple DES) encryption engine.

HDDKEY is an operating system independent and does not require any software drivers. It works on the hardware layer without software intervention of any kind. The secret random number transferred from your key token never reaches RAM or HDD surface where your sensitive data are stored in the encrypted form. The secret key is erased from its internal registers upon reset, reboot or shut down and can never be recovered.

HDDKEY is offered in 128 and 192 bit secret key strength.



Depending on the key strength of the controller you got, the device will take 128 or 192 bits from external serial EEPROM respectively.

Your secret KEY number is stored in the small external memory device called the secret key token. The user is advised to hide one small memory device token in a safe and secret repository and use only one secret key token at a time.

It is strongly recommended to hide the second key token outside your house, work or a place you often visit.

Until your secret key token is in your hands then your hard disk is secure from intruders and thieves. If you lose both of your secret key tokens your data is gone forever. If your HDDKEY crypto controller (not the token) fails then nothing wrong happens. Simply replace the controller with a new one of the same encryption strength and use your old key tokens to access your data. Your key tokens need to be connected only for booting the computer. You can disconnect them right after your operating system was loaded. Remember to reconnect them before rebooting or starting the computer.

HDDKEY uses the 93C46 standard serial EEPROM memory integrated circuit as your security key. The 93C46 must be configured in the 16 bit mode of operation by connecting the pin6 (ORG) to the positive power supply pin8 +5V for proper operation. You can use any other device as your secret key storage medium because it uses industry standard 93C46 transmission protocol.

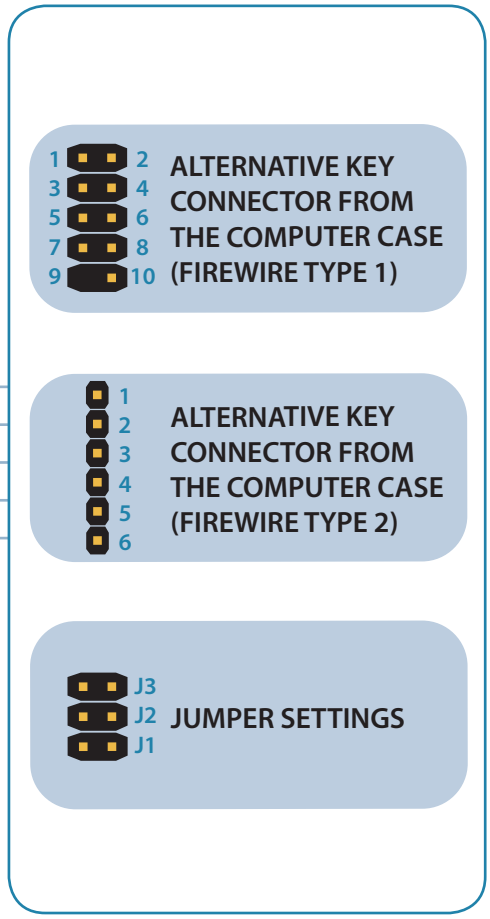
Each HDDKEY crypto controller is equipped with two key tokens with preprogrammed random numbers. The user is strongly advised to reprogram these tokens himself. Please use the attached 3des_v2.6.exe file to generate your own random numbers. Use any serial EEPROM programmer to program your newly generated numbers to your tokens. Nobody keeps copies of preprogrammed random numbers but please reprogram them for your safety. Distributors shall not help the end user to reprogram key tokens. Distributors shall not help to install the device. Distributors shall not wipe hard drives of their customers. The user must do all of this on his own.

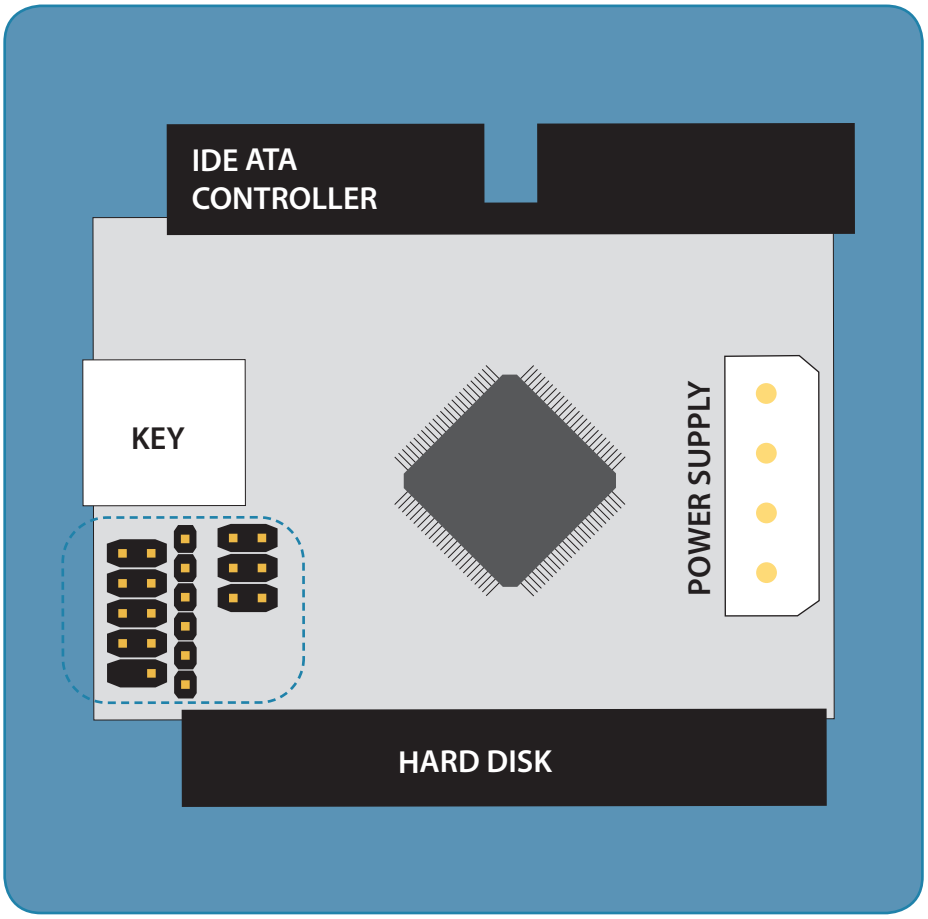
The device is specially designed to guard the private property, small business and corporate property against jealous spouses, business competitors or thieves and is not intended to be used in any Government, Police or Military institutions. The device does not have certificates of any kind in order to be used in Government, Police or Military and shall not have such certificates in the future. The sensitive nature of the cryptography of the HDDKEY may be subject to some export control regulations and other cryptography related laws in the country you live in. Be aware that export to some countries is prohibited by the law. Please follow your country's legal acts for details.

revolutionary device
intended to encrypt
in real time,
the entire hard disk content,
on the fly

INSTALLATION

1. Installation Overview





HDDKEY
is an operating system independent
and does not require any software drivers.

2. System Configurations

There are five alternate connections of the HDDKEY with the Motherboard and the hard drive. As shown in the Image 1, typical configuration is comprised with only one IDE device in either one of the two IDE channels supported by the IDE host controller. The drive controlled by the HDDKEY is fully encrypted.

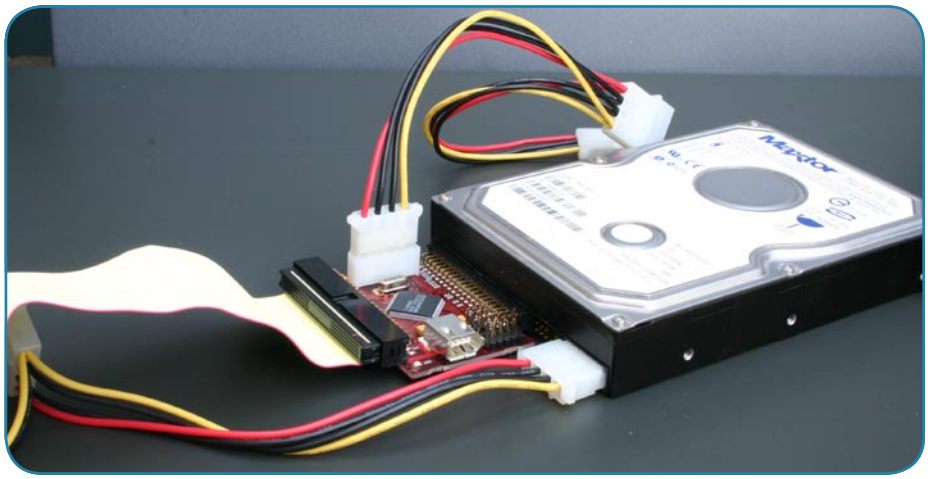


Image 1.
The single hard drive in the system.

The other possibilities are shown in **Image 2**, **Image 3**, **Image 4** and **Image 5**. You cannot connect two HDDKEY encrypted hard drives to the same IDE controller. The drive controlled by HDDKEY is fully encrypted. However, the drive that is positioned in front of the HDDKEY stores only clear text and is therefore an unencrypted drive. Encrypted and non-encrypted text may be exchanged by simply dragging and dropping files. You can use one HDDKEY encrypted disk and the CD/DVD drive in the same IDE channel but of course your DVD will not be encrypted. You must not attach the HDDKEY to the CD/DVD.

In other words there can be only one HDDKEY controlled hard disk on one IDE cable.

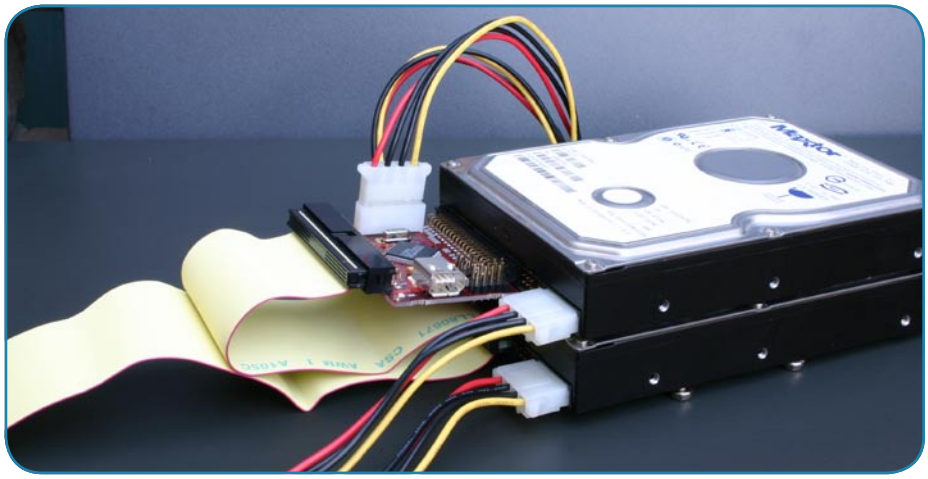


Image 2.
Master drive encrypted,
Slave drive not encrypted.

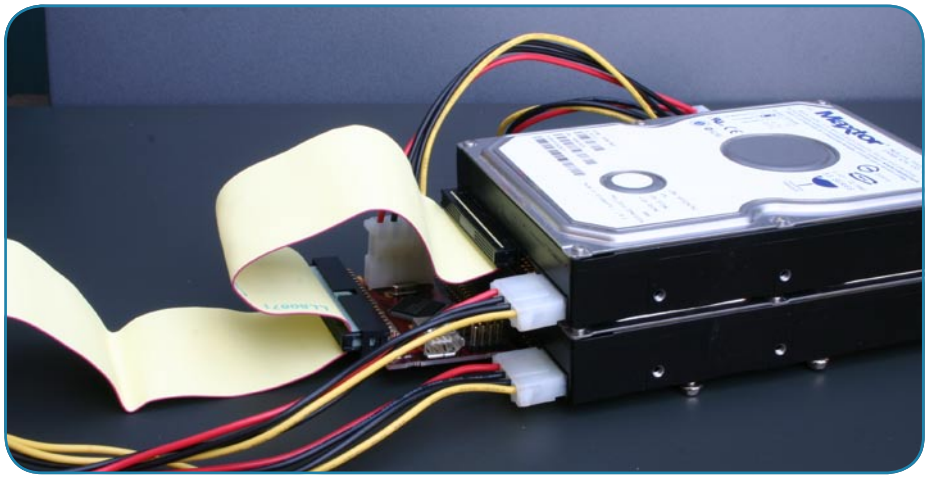


Image 3.
Slave drive encrypted,
Master drive not encrypted.

Image 4.
Slave drive encrypted
with master DVD recorder.

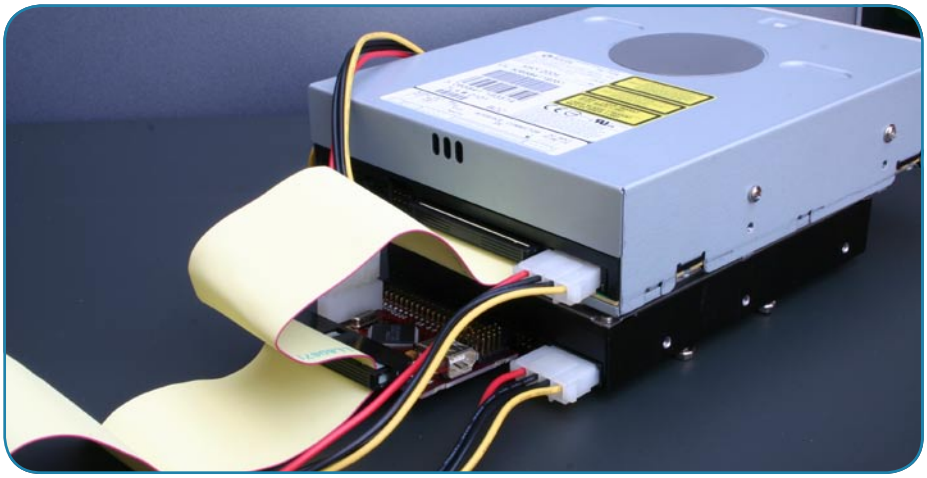
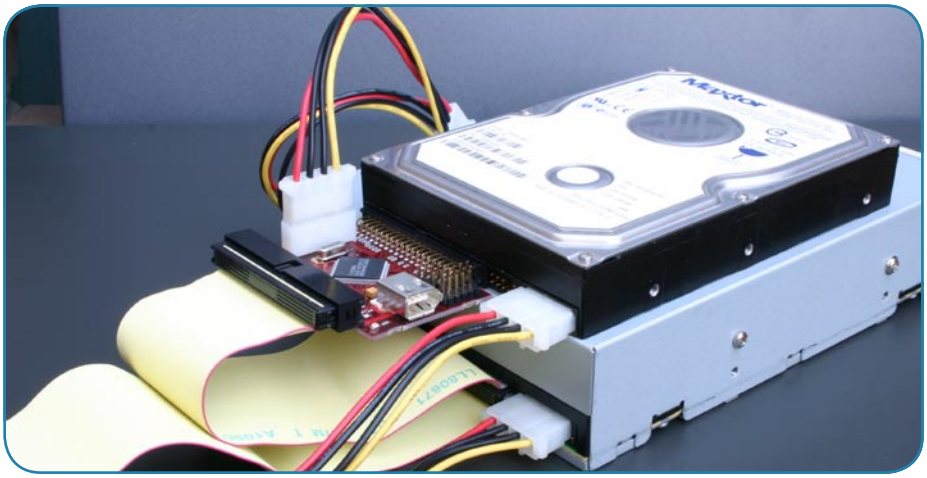


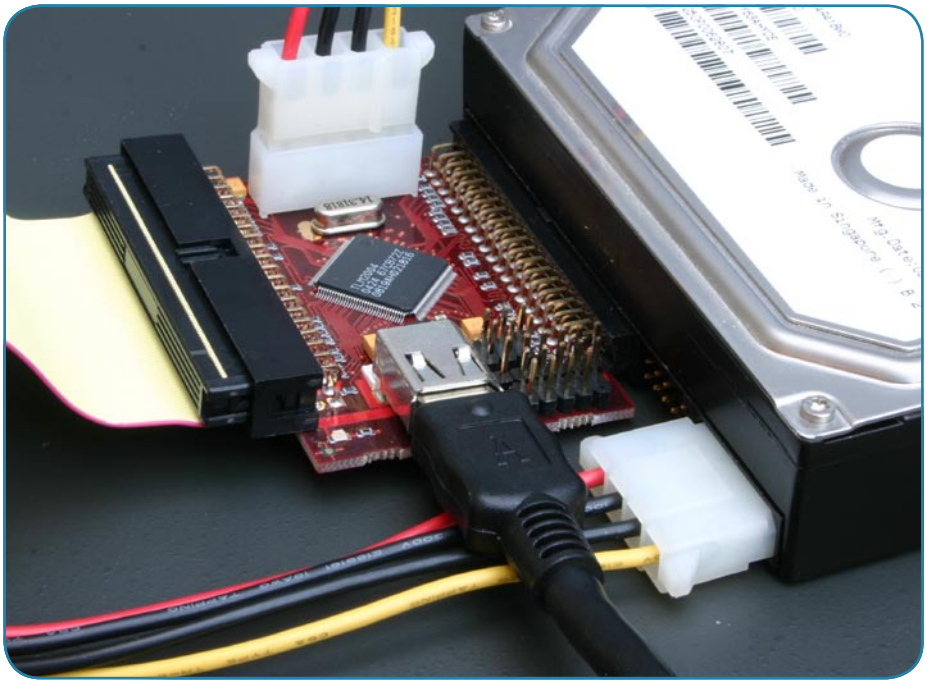
Image 5.
Master drive encrypted
with slave DVD recorder.



3. Connecting the KEY token

There are three possibilities to attach the secret key token.
Connect a cable directly as on the image below:

Image 6.



Your secret KEY number is stored in the small external memory device called the secret key token.

The user is advised to hide one small memory device token in a safe and secret repository and use only one secret key token at a time.

Older FireWire 6pin connector sometimes spotted in the computer hardware. The pin number ONE is marked at the bottom of the printed circuit board of the HDDKEY. Connect a cable from your computer's cabinet to the pins on the HDDKEY as follows:

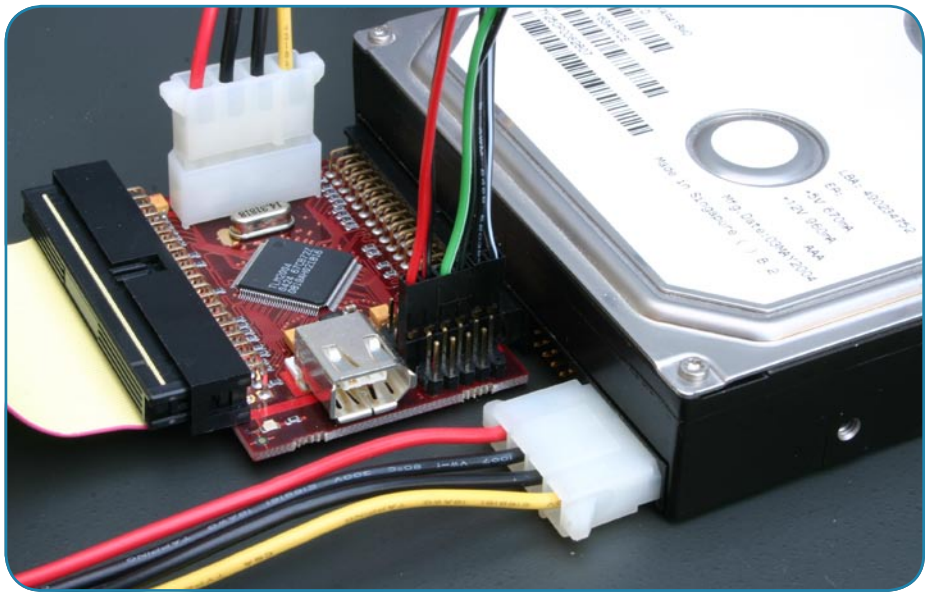


Image 7.

The FireWire-type connector widely used on motherboards. The pin number ONE is marked on the top of the printed circuit board of the HDDKEY. Connect a cable from your computer's cabinet to the pins on the HDDKEY as follows:

Image 8.

Image 9.
Key tokens.

Until your secret key token is in your hands then your hard disk is secure from intruders and thieves.

protect your data

The HDDKEY does not have any recovery feature so if you lose all of your secret key tokens then

your data will be lost forever.

4. Preparing drives

If you intend to use a newly purchased and never used hard drive you don't need to follow the described procedure.

If you want to use your hard drive which already contains your files and you plan to use it with HDDKEY, then the procedure is more complicated as far as security reasons are concerned.
If you want to securely hide the content of your disc you need to:

1. Make a backup of your files to a DVD-R or CD-R.
2. Securely wipe the entire content of your hard drive by overwriting it several times.

It can be done by any piece of software like PGP. You can obtain a free copy of PGP from www.pgpi.com.
It is not trivial to do it properly. You need to use 2 hard disks for this purpose. At least one HDD with an operating system and PGP plus the second HDD which we will wipe. This second drive will be securely wiped and then converted to the encrypted HDD after installing the HDDKEY.

Assuming you have two temporary hard drives installed, simply quick format the second drive to ensure it is empty and then use PGP to "wipe the free space" on that second drive. Again, the second drive has to be empty. Please read the PGP manual or search the internet for securely wiping the hard disk contents. It is not enough to wipe only the free space on your HDD where you boot your operating system from. You need to wipe everything and especially the place where the operating system was previously stored.

Please note that the HDDKEY will encrypt everything that was written after the HDDKEY installation. It will not encrypt or convert your old system installation to the encrypted volume.

Of course if you don't have sensitive data on your disc you don't need to wipe it at all. In general it is up to the user how he handles his sensitive or not sensitive data. You must decide.

3. Attach the HDDKEY to the previously wiped disc.
4. Install the operating system or whatever you want.
5. Physically destroy DVD-R or CD-R used for temporary backup.

From now you are secure!

Until your secret key token is under your possession you are safe.

The HDDKEY does not have any recovery feature so if you lose all of your secret key tokens then your data will be lost forever.

5. More HDDKEY devices and only one secret key token

You can easily use more than one HDDKEY in the same computer with only one key token. To do these please follow one simple rule.

All HDDKEY devices must be set to the same ULTRA ATA mode regardless of the drive's capability.

For example if you have 2 drives, one drive is ATA-133 and the second drive is ATA-100. Set both HDDKEY units into ATA-100 by populating appropriate jumpers and only jumpers. Please do not change anything in the BIOS setup of your PC.
The difference between ATA-133 and ATA-100 is not noticeable and is under the perception level.
Now you can connect a key token cable from the enclosure's external socket or normal FireWire cable to the one HDDKEY of your choice.
The second HDDKEY must be connected together with the first one with a 4 wire cable as follows:

USE the 6pin header socket which is normally used for a key token to connect an external FireWire socket inside your computer cabinet (enclosure). Make a simple ONE to ONE bridge

between devices. You can do the same if you connect three or four HDDKEY controllers in your computer system by bridging them together using a piece of wire with appropriate plugs. Your normal key token can be connected to any HDDKEY in the chain.

The 6pin header socket

Pin number	HDDKEY 1		Pin number	HDDKEY 2
1	do not use		1	do not use
2	do not use		2	do not use
3	93C46 EEPROM data output	<==>	3	93C46 EEPROM data output
4	93C46 EEPROM data input	<==>	4	93C46 EEPROM data input
5	93C46 EEPROM clock	<==>	5	93C46 EEPROM clock
6	93C46 EEPROM chipselect	<==>	6	93C46 EEPROM chipselect

Be careful doing this because improper pin connection can blow up your computer.

Please note that the HDDKEY will encrypt everything that was written after the HDDKEY installation. It will not encrypt or convert your old system installation to the encrypted volume.

SPECIFICATION

- ULTRA ATA (UDMA) 66, 100 and 133
- TDES, TRIPPLE DES, 3DES Data Encryption Standard
- BURST speed 133MB/s
- POWER led
- KEY ACCEPT LED must not flash during the normal operation when a key token was accepted

10 pin secret key header on the HDDKEY controller board.

Pin number	HDDKEY Pin description	FireWire Pin Description
1	93C46 EEPROM chipselect	TPA+
2	93C46 EEPROM clock	TPA-
3	93C46 GND (ground)	GND
4	GND (ground)	GND
5	93C46 EEPROM data input	TPB+
6	93C46 EEPROM data output	TPB-
7	93C46 +5V power supply	+5V (VCC)
8	+5V power supply	+5V (VCC)
9	Not populated	Not populated
10	GND (ground)	GND

6 pin secret key header on the HDDKEY controller board.

Pin number	HDDKEY Pin description	FireWire Pin Description
1	+5V power supply	+5V (VCC)
2	GND (ground)	GND
3	93C46 EEPROM data output	TPB-
4	93C46 EEPROM data input	TPB+
5	93C46 EEPROM clock	TPA-
6	93C46 EEPROM chipselect	TPA+

IEEE-1394 (FireWire) female socket on the controller board.

Pin number	HDDKEY Pin description	FireWire Pin Description
1	+5V power supply	+5V (VCC)
2	GND (ground)	GND
3	93C46 EEPROM data output	TPB-
4	93C46 EEPROM data input	TPB+
5	93C46 EEPROM clock	TPA-
6	93C46 EEPROM chipselect	TPA+

Please note that standard 6/6 FireWire cable is a crossover cable so TPA and TPB pairs are swapped. The secret key's female socket has also TPA pair swapped with TPB pair.

Power supply socket on the HDDKEY controller board.

Pin number	HDDKEY Pin description
1	+5V power supply
2	GND (ground)
3	GND (ground)
4	+12V power supply

Jumper settings
on the HDDKEY controller board.

Jumper number	HDDKEY Pin description
JP1	MASTER=OPEN SLAVE=CLOSED
JP2, JP3	ULTRA ATA mode

ULTRA ATA jumper settings
on the HDDKEY controller board.

Pin number	ULTRA ATA-66	ULTRA ATA-100	ULTRA ATA-133
JP2	OPEN	CLOSED	OPEN
JP3	CLOSED	OPEN	OPEN

The HDDKEY supports ULTRA DMA mode (ULTRA ATA) only. If used in MwDMA mode (Multi Word DMA mode) the data on your hard drive will be corrupted. Please be sure to have the proper ULTRA DMA mode setting or AUTO setting in the Bios SETUP of your computer. Normally all BIOS settings are set to AUTO and it is the best. Don't change it manually and don't play with DMA settings in the BIOS Setup of your PC.

In case of the data corruption caused by a virus or a simple operating system failure please recover your data in the usual way with the HDDKEY present in your computer and with your proper key token. Even if you have corrupted data on your hard drive you can recover them. Your corrupted data will only be visible through the HDDKEY and only with your proper key token because any bit on your drive, corrupted or not is still strongly encrypted by the device and your secret key.

Before you start using HDDKEY be sure to screw your hard drive to the metal compartment of the computer enclosure. Only the proper electric grounding of your drive will ensure stable operation.

Avoid using cheap and low quality IDE cables.
Use only 80 conductor cables.
Poor quality cables can cause installation problems.